North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

Nearly 150 residents displaced by a massive apartment fire. Authorities got the call around 5:45 tonight and the fire quickly spread, turning into a 4 alarm fire. Fargo's fire marshal says the fire started on the first floor, possibly because of a grill. It moved up, igniting propane tanks. The entire roof of the building is gone. Authorities say it was tough to get water up to the attic. Authorities believe everyone did get out of the complex. So far, no serious injuries reported. The apartment's property manager spotted the fire and called 9-1-1. Source: http://www.wday.com/event/article/id/39475/

Regional

(Minnesota) **Emergency exercise establishes roles.** Communication is key when it comes to emergencies. This was identified as the main area to focus on at a recent tabletop exercise conducted by the Hubbard County< Minnesota emergency manager. Many representatives from law enforcement, first responders, fire department, and other agencies attended. The scenario for the mock exercise was that a propane storage tank explodes at the AmeriGas stockyard in Park Rapids and resulted in a fire and aftermath explosions sending flaming debris to the nearby Cenex agricultural fertilizer storage plant and Gas Service Company, igniting a secondary fire. All fires were sending a plume of smoke and toxins into the air drifting toward Park Rapids, causing a partial evacuation. Propane tanks continued to explode, burn and ignite, fueling the fire. The scene of the mock fire was within 1,000 feet of the Park Rapids Fire Department, which sustained damage, and mutual aid was requested from the Nevis Fire Department due to the loss of one fire engine. Source: http://www.parkrapidsenterprise.com/event/article/id/25599/

(Minnesota) **Correctional officers union warns of 'dangerous staffing crisis' in Minnesota.** Tired of deep funding cuts at Minnesota's state prisons, union correctional officers allege a "dangerous staffing crisis" that could lead to more trouble as inmates test authority. Concerns over adequate staffing at Stillwater prison haven't been resolved since a violent May 15 disturbance involving about 70 inmates who live in the B West cellhouse, said a spokeswoman for the American Federation of State, County and Municipal Employees (AFSCME) Council 5, the union that represents about 1,900 corrections officers at Minnesota's eight state prisons. "We figure it's just a matter of time before someone gets hurt," she said October 11. "The staffing shortage has created danger and puts both the staff and the public at risk." The Stillwater prison hasn't added "a single correctional officer" in the past several years, while the prison's population has grown by 400 inmates, the union said in a statement. To guard 1,610 inmates, the prison has 61 officers on the day shift, 59 in the evening and 21 overnight, the union said. Source: http://www.grandforksherald.com/event/article/id/179058/group/homepage/

(South Dakota) **Drill keeps Sioux Falls students safe.** Sioux Falls, South Dakota Christian Middle School students were involved in South Dakota's first reunification drill October 13. The drill

simulates a school lock-down, evacuation, and the reuniting of parents with their child. The drill began with police holding a simulated press conference detailing a situation involving a gunman at the school. Swat members were called on scene and escorted students out of the school and into an armored truck. Students were then transferred to the University of Sioux Falls stadium parking lot to be screened by police, and then placed on a bus to be sent to the undisclosed reunification point and finally meet up with their parents. Several different law enforcement agencies were involved in the drill, which was sponsored by a $40,000 homeland security grant, and the school's principal hopes te drill is used as a model. Police and emergency management officials will spend the next couple of days rating the drill. Source: http://www.ksfy.com/Global/story.asp?S=13319631

(South Dakota) **South Dakota governor relaxes transportation rules on petroleum products.** Due to extremely low inventories and outages of petroleum fuels in South Dakota, the governor has issued an executive order to continue expedited commercial delivery of fuel for the next several days. The governor said transportation of gasoline, diesel, and propane is in high demand for agriculture production needs. The order assures farmers that fuel supplies are maintained to help continue normal agricultural operations. The governor's executive order declares a state of emergency and exempts delivery of petroleum products from federal motor carrier regulations on drivers' hours of service. Although hours of service have been temporarily suspended for commercial deliveries, companies may not require or allow fatigued drivers to make delivers. The executive order, issued October 12, expires at midnight, October 31. Source: http://www.rapidcityjournal.com/news/article_79a966e4-d652-11df-8313-001cc4c002e0.html

National

(Arkansas) **Swarms of earthquakes hit central Arkansas.** Central Arkansas has been hit by a series of earthquakes recently, the biggest being a magnitude 4.0 that shook the town of Guy, about 150 miles west of Memphis, Tennessee. A research scientist from the University of Memphis said Arkansas is getting many unusual earthquakes, more than 60 in the last month. "In the New Madrid Seismic Zone, there's approximately 200 per year, so if we had that many in Central Arkansas in less than a month, something is going on," the scientist said. That part of central Arkansas isn't even part of the New Madrid Fault Zone, so researchers are trying to determine what's causing the earthquakes. The scientist thinks they may be the result of injecting salt water into old natural gas wells to force more gas production. Even though the two areas are not connected, his biggest worry is along the New Madrid fault where damage from a magnitude 6.0 earthquake could be catastrophic. "A probability of having that in a 50-year period is about 25 to 40-percent chance," the scientist said. There have been no reports of damage or anyone getting hurt from the earthquakes. Source: http://www.myeyewitnessnews.com/news/local/story/Swarms-of-Earthquakes-Hit-Central-Arkansas/UpIqQoKMgEKYVpCn3JQ5qA.cspx

International

Stuxnet spreads to Finland. Corporate espionage is spreading in Finland, and the country was recently targeted by the infamous Stuxnet worm, Finnish newspaper Helsingin Sanomat reports. The complex malware has been found in at least one institution that uses the industrial equipment targeted by the worm. It has not caused any damage. In addition, Finnish state institutions have also

been attacked. According to the Finnish Security Police, spyware has been spreading both through e-mail and via USB flash drives. Source: http://www.thenewnewinternet.com/2010/10/14/stuxnet-spreads-to-scandinavia/

9 British Columbia dams at 'high risk' of failing: audits. Nine British Columbia, Canada dams have recently been found at "high risk" of failing, including a large dam near the southern B.C. community of Greenwood, Postmedia News has learned. And the British Columbia Ministry of Environment audits of the 2,000 dams in B.C. found that of the nine "high risk" dams, five of them are additionally classified as "high consequence," meaning they could cause significant damage if they failed. The information was released the week of October 4 in response to a freedom of information request filed by the Vancouver Sun, following the collapse in June of the Testalinden Lake dam, which caused extensive damage to 14 private properties in Oliver, British Columbia. A senior ministry official said most maintenance and inspection concerns have been addressed with the nine dams, and insisted no one living near them should be afraid. Source: http://www.nationalpost.com/news/canada/dams+high+risk+failing+audits/3668841/story.html

Comm Games ups security after terror threat report. The security clampdown at the Commonwealth Games in New Delhi went into overdrive October 13, a day ahead of the closing ceremonies, as reports emerged overnight of a potential terror threat. London's Daily Mail reported that Indian intelligence had warned of a militant terrorist plot to attack Delhi October 14. The report cited unconfirmed intelligence indicating that the Pakistan-based Lashkar e Taiba group, which carried out the Mumbai attacks in 2008, was targeting the Indian capital on the day of the closing ceremonies. The week of October 4, the Indian military and police seized 10 improvised explosive devices hidden in wooden boxes in Jammu city, an army officer told the Associated Press. Jammu is roughly 360 miles north of Delhi, and the officer said the destination for the explosives was not immediately known. The explosives were seized from four people, who have been arrested. The Commonwealth Games Federation president said he was unaware of any "new, credible, specific terror threat." Source: http://www.google.com/hostednews/ap/article/ALeqM5iLjAZVmy9BFpTv7_7qOmPS4YvGkwD9IQPU9G0?docId=D9IQPU9G0

Workers building emergency dams to stem second toxic spill. Workers in Hungary were racing October 12 to build three emergency dams to stem an expected second toxic spill from an aluminum plant. Some 500,000 cubic meters of toxic red sludge is in the plant's reservoir, whose wall shows signs of ruptures and cracks, said a spokeswoman with Hungary's emergency services department. Officials say it is only a matter of time before the wall breaks and spews the sludge across the landscape. The amount of sludge that remains in the reservoir is about half the amount that spilled out a week ago, inundating three villages, killing eight people, and leaving the landscape covered in red. It was not clear when the emergency dams would be finished. Officials had said the dams would be finished by the morning of October 12, but later they pushed it back to the morning of October 13. Crews were also trying to remove a layer of liquid from the top of the sludge in the reservoir in order to make the mud less mobile if the wall breaks. The head of the company that owns the plant was arrested, accused of public endangerment and harming the environment, authorities said. About 800 people have been evacuated from the village of Kolontar, downstream from the reservoir, and hundreds of soldiers were ready to rescue inhabitants of a nearby village if the wall collapses. Source: http://www.cnn.com/2010/WORLD/europe/10/12/hungary.toxic/

Tanker, container ship collide in North Sea. A Greek tanker collided with a container ship 20 miles off the Dutch coast October 12 and briefly leaked jet fuel into the North Sea. The crew of the Mindoro pumped the remaining fuel into an undamaged part of the ship, ending the leak, a Coast Guard spokesman said. "We have a small slick in the water, but it is minimal and it is evaporating very quickly," he said, adding that it was unclear how much jet fuel had spilled into the sea. Offshore winds were blowing the slick away from the coast. "The situation appears to be under control," he said. The spokesman said an oil spill control boat was on its way to the stricken tanker as a precaution. A coast guard tug boat also was heading to the scene. No one was injured on either of the ships. The Mindoro dropped its anchor and was waiting for experts to investigate whether it was safe for it to return to port. The tanker had a 16-foot-wide hole torn in its hull close to the waterline. The container ship involved in the collision, the Cypriot-flagged Jork Ranger, was returning to port, but was not seriously damaged. It was not immediately clear how the collision happened. Cypriot and Greek authorities were discussing who will head an investigation since the collision occurred in international waters. Source: http://www.foxnews.com/world/2010/10/12/media-tanker-leaking-kerosene-north-sea/

Banking and Finance Industry

Financial services firm turning to a private cloud. Munder Capital Management, a Birmingham, Michigan-based firm that manages $13 billion in assets, is turning to a private cloud after determining public cloud technologies are not yet ready to meet its needs. A network operations and virtualization engineer at Munde said the firm felt public clouds are not yet a good option because of regulatory issues around the control of data, a lack of adequate service level agreements with cloud providers, and an absence of standard agreements that "allow freedom of movement between providers." The engineer also cited a lack ofIT control when a company relies on public cloud services. "We really don't want to be in a position to have to shrug and say 'I don't know' when a system is running slowly," he said at the Storage Networking World conference. Munder decided to create "a private cloud that has many of the same characteristics of a public cloud but with much higher control, security and availability," the engineer said. Research firm IDC projects the cloud computing market will grow from $23 billion today to about $55 billion in 2014, but much of the growth so far has been in new hosted services, an IDC analyst said. Source: http://www.computerworld.com/s/article/9190878/Financial_services_firm_turning_to_a_private_cloud

Credit-card crime up as unemployment climbs. Credit-card crime is soaring to unprecedented levels in the United States, with a 32 percent rise in the amount of fraudulent attempts to buy goods online, by mail order, or by phone in the first half of this year, and a payment fraud prevention company predicts the continuing rise in unemployment and the increasing ingenuity of fraudsters are partly to blame. Crooks with stolen or cloned cards prefer to use them in situations where the cards do not have to be physically handed over, making e-commerce sites constant –- and perfect –- targets for scammers. "In the first 6 months of 2010, our figures show that attempted ecommerce payment fraud reached an estimated value of $1.14 billion," said the CEO of Retail Decisions. "We predict this could reach $2.83 billion by the end of the year –- increasing by 32 percent compared to the $2.14 billion total recorded in 2009." In contrast, the fraud situation seems to be improving in the U.K., where the market is predicted to see a 12 percent decrease this year, thanks to industry initiatives

such as chip and PIN, and the increasing use of sophisticated fraud-detection tools by retailers and banks. “This is a stark warning for U.S. merchants and consumers to protect themselves against payment fraud,” the CEO said. “Merchants must ensure they have a dynamic fraud-prevention solution in place that can adapt quickly to changes in the way fraudsters operate.” Source: http://www.thenewnewinternet.com/2010/10/12/credit-card-crime-up-as-unemployment-climbs/

PCI compliance means getting your app security together. Many companies’ applications still do not meet the security standards outlined in the Payment Card Industry (PCI) Data Security Standards, according to a recent study. During the 18-month study, which was published the week of October 4, security firm Veracode scanned the binary code of more than 2,900 applications on behalf of its clients. Its findings are sobering: Nearly six out of every 10 applications had an “unacceptable” level of security; more than eight out of 10 applications failed to catch classes of Web application vulnerabilities required for remediation under PCI DSS. While the customers eventually fixed the flaws, most enterprises’ applications fail to meet with PCI standards — a rather low bar for Web application security said the senior director of security research at Veracode. “These [enterprises in the study] are the organizations that are proactive about security,” the official said. “These are the ones that decided, yes, we are going to scan our applications and try and figure out what the vulnerabilities are and fix them. There are other organizations out there that are not going to scan and are not doing anything as far as security is concerned.” Source: http://www.darkreading.com/vulnerability_management/security/management/showArticle.jhtml?articleID=227701216

States to probe mortgage mess. A coalition of as many as 40 state attorneys general is expected October 13 to announce an investigation into the mortgage-servicing industry, an effort some of them hope will pressure financial institutions to rewrite large numbers of troubled loans. The move comes amid recent allegations that mortgage-servicers, which include units of major banks such as Bank of America Corp., submitted fraudulent documents in thousands of foreclosure proceedings nationwide. The banks say the document problems are technical — largely the result of papers approved by so-called robo-signers with little review — and do not reflect substantive problems with foreclosures. The attorneys’ general immediate aim is to determine the scale of the document problems and correct them. But several of them have said that the investigation could force the lenders and servicers to agree to mass loan modifications or principal forgiveness schemes. Other possibilities include financial penalties or changes in mortgage servicing practices. Source: http://online.wsj.com/article/SB10001424052748704518104575546512922974100.html?mod=WSJ_RealEstate_LeftTopNews

Foreclosure logjam threatens Fannie, Freddie. A breakdown in the nation’s foreclosure process threatens to create billions of dollars in losses for federally controlled mortgage finance companies Fannie Mae and Freddie Mac, highlighting how improper actions by banks could impose new costs on taxpayers, said government officials and industry sources. In letters and in a conference call October 7, Fannie and Freddie told the lenders they would be on the hook for any losses the two mortgage companies might suffer as a result of flaws in the foreclosure process. Freddie has set a deadline of October 11 for banks to respond, according to the letter. The interim director of the Federal Housing Finance Agency said the two firms are trying to come up with a “tailored approach” to the debacle. In some of these meetings, administration officials have expressed concern about whether a nationwide moratorium on foreclosures would damage not only Fannie and Freddie but the fragile housing

market as well. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/10/11/AR2010101106693.html

Massive phishing attack zones in on iTunes users. PandaLabs has discovered that iTunes has become a major target for hackers looking to steal credit-card data from the millions of users. Victims receive an email informing them they have made an expensive purchase on iTunes. The user, who has never made the purchase, is concerned by the email and tries to solve the problem by clicking on the fake link. After clicking the link, the victim is asked to download a fake PDF reader. Once installation is complete, the user is redirected to an infected Web page containing the Zeus Trojan, which is designed to steal personal data. This phishing attack was uncovered shortly after a similar phishing attack targeting LinkedIn users, which appears to have originated in Russia. This technique has been reported to the Anti-Phishing Working Group, which has started to block some of the Web addresses linked to in the fake email. Source: http://www.thenewnewinternet.com/2010/10/12/massive-phishing-attack-zones-in-on-itunes-users/

Chemical and Hazardous Materials Sector

(Arizona) **Deputy: Suspicious device found at nuclear plant west of Phoenix was probably smoke flare.** A device that caused the entrance to a nuclear power plant west of Phoenix, Arizona to be closed appears to be a smoke flare used in firefighter training, authorities said. The device was found under the seat of an employee's car at a security checkpoint 1 mile from the Palo Verde Nuclear Generating Station at about daybreak October 13, a Maricopa County Sheriff's Office spokesman said. At first glance, it looked like a stick of dynamite, so plant security closed the checkpoint to traffic as a precaution. Power plant operations were not affected and the checkpoint was reopened after about 3 hours. The employee was questioned but the spokesman said she was not arrested. An official with plant operator Arizona Public Service Co. (APS) said the issue will likely be handled as an internal matter. The device was 4 to 6 inches long and had a fuse attached, said the vice president for nuclear operations at APS. The spokesman said it had "smoke" written on it.Source: http://www.chicagotribune.com/business/sns-ap-us-nuke-plant-suspicious-packages,0,4783536.story

Implementation guidance for physical protection of byproduct material category 1 and category 2 quantities of radioactive material. On July 14, 2010, the Nuclear Regulatory Commission (NRC) noticed for public comment implementation guidance for a proposed rule to establish security requirements for the use and transport of Category 1 and Category 2 quantities of radioactive material. The public comment period for this guidance was to have expired November 12, 2010. The NRC received several requests to extend the comment period to January 15, 2011. Due to the size and complexity of the draft implementation guidance, and the associated proposed rule, NRC officials announced in an October 13 Federal Register notice that they have decided to extend the comment period until January 18, 2011. Source: http://edocket.access.gpo.gov/2010/2010-25784.htm

Physical protection of irradiated reactor fuel in transit. The Nuclear Regulatory Commission (NRC) has proposed amendng its security regulations pertaining to the transport of irradiated reactor fuel (for purposes of this rulemaking, the terms "irradiated reactor fuel'" and "spent nuclear fuel" (SNF) are used interchangeably). This proposed rule, published in the October 13 Federal Register, would

establish generically applicable security requirements similar to those previously imposed by NRC orders issued after the terrorist attacks of September 11, 2001. The rule would establish the acceptable performance standards and objectives for the protection of spent nuclear fuel shipments from theft, diversion, or radiological sabotage. The proposed amendments would apply to those licensees authorized to possess or transport spent nuclear fuel. The security requirements would also address, in part, a petition for rulemaking from the State of Nevada (PRM-73-10) that requests that NRC strengthen the regulations governing the security of spent nuclear fuel shipments against malevolent acts. The comment period expires January 11, 2011. Comments specific to the information collection aspects of the rule are due by November 12, 2010. Source: http://edocket.access.gpo.gov/2010/2010-25392.htm

COMMERCIAL FACILITIES

(Florida) **Central police have person of interest in bomb blast.** Central, South Carolina police said they have a person of interest in connection with a bomb that exploded under a car at an apartment complex. Residents of the Summit at Cross Creek Apartments said the blast rattled windows October 14. A resident said he was in his kitchen when the device detonated. "It was basically like a shotgun that went off," he said. "I heard this loud explosion and it sort of rumbled." Investigators said someone planted a bomb near the back tire of a 2007 Honda Civic. They said the blast blew off the bumper and scattered debris throughout the parking lot. "We heard it all the way up here," said the Central police chief. The Central Police Department is about 500 feet away from the apartments where the explosion happened. The chief said moments after the blast, dozens of 911 calls were made. He also said what is left of the explosive device is now being analyzed in an effort to determine what kind of bomb it was. Source: http://www.foxcarolina.com/news/25397702/detail.html

(New York) **As terror alert continues, NYPD holds drill to prep for Mumbai style attack.** As U.S. officials proclaim an alleged European terror plot still active, New York City police conducted a drill October 14 that simulated a Mumbai, India-style attack on civilians on a crowded street in Manhattan's financial district. The drill simulated an attack near Wall Street and Ground Zero, on a mock block that contained a department store, a hotel, and a federal regulatory agency. The New York police commissioner addressed the media before the drill which began with two large explosions. "This is what we do," he explained. "We think the unthinkable." The drill simulated multiple bombs and shooters, including a bomb under a vehicle, and police responded with helicopters, dogs, automatic weapons, and an armored car. In the immediate aftermath of the 2008 Mumbai assault that claimed 175 lives, the New York Police Department (NYPD) revised its tactics to deal with a terrorist commando assault. During October 14's drill in the Bronx, heavily armed Emergency Service Unit officers were backed by officers from the Organized Crime Control Bureau (OCCB) trained to respond to such an attack. The OCCB officers are intended to beef up the NYPD response and prevent multiple simultaneous attacks from overwhelming the responding force. Source: http://abcnews.go.com/Blotter/terror-alert-continues-nypd-holds-drill-prep-mumbai/story?id=11879452

(Virginia) **Two men arrested in Rocky Mount Walmart bomb threat.** Two men face charges in connection with a bomb threat at the Rocky Mount, Virginia Walmart October 12. Rocky Mount Police said a 20-year-old and a 19-year-old called in a bomb threat around 10:34 p.m. Officers evacuated the Walmart, then called for bomb sniffing dogs from state police, the Virginia Tech Police

Department, and the Pulaski Police Department to search the store. The dogs did not find any explosives. A Rocky Mount Police lieutenant and sergeant investigated the bomb threat, and believe the threat was connected to a cell phone that was stolen earlier October 12. Source: http://www2.wsls.com/news/2010/oct/13/two-men-arrested-rocky-mount-walmart-bomb-threat-ar-561133/

(Louisiana) **Businesses evacuated after Hazmat spill.** The driver of an 18-wheeler told police he noticed his load shift, and then pulled over in this Sutherlands parking lot on Mansfield Road and 70th in Shreveport, Louisiana where he noticed a leak. Emergency officials determined that the liquid dripping onto the pavement was corrosive. "It can do some damage to the flesh as a vapor," said the chief safety officer for the Shreveport Fire Department. A drain was situated in the middle of the parking lot, a pathway to the city's water system. Emergency officials said that when the hazmat team arrived, the material was just 3 feet from that drain. "The environment is another big concern," said the chief safety officer. "Which is why we immediately began damming the product as soon as we got on scene to prevent it from getting in any ditch or any drainage inside this parking lot." Source: http://www.ksla.com/Global/story.asp?S=13320512

(Connecticut) **Woman threatens to blow up Walmart in Old Saybrook.** A 34-year-old Old Saybrook Connecticut woman was arrested and the Walmart in Old Saybrook was evacuated October 13 after the woman passed a pharmacist a note threatening to blow up the store if her prescription for amphetamines was not filled, police said. No explosives were found in the store and no one was hurt. But police said the woman's car contained a gas can with wires coming out of it and separately wires coming from the fuse panel wrapped around the steering column and entering back into the engine compartment. After being called by the pharmacist, the first arriving officers confronted the woman. After being noncompliant, she was taken into custody without injuries, police said. Source: http://middletownpress.com/articles/2010/10/14/news/doc4cb7114f464d2099375096.txt

(Indiana) **WL's State St. reopens after bomb threat.** A bomb threat briefly shut down much of the Village area in West Lafayette, Indiana, the night of October 9. According to West Lafayette police, someone phoned in a vague bomb threat to the Dominos Pizza on Salisbury Street around 6:45 p.m. Police evacuated the restaurant, some nearby businesses and shut down much of State Street, Chauncey Street and some nearby alleys for about 30 minutes while a bomb-sniffing dog searched the area. The closure came just as crowds were starting to file into the near-campus bar and restaurant district to catch the 7 p.m. kickoff for the Purdue-Northwestern football game. After no bomb was discovered, police opened things up again around 7:25 p.m. According to a West Lafayette police sergeant, police will try to locate the suspect and press charges. "We'll have to look at every avenue of what's going on before we decide on charges," he said. Source: http://www.jconline.com/article/20101009/NEWS09/101009017/UPDATE--WL-s-State-St.-reopens-after-bomb-threat

(District of Columbia) **Terror threat to restaurants as Al Qaeda calls for attacks on government workers in D.C.** The terror group tied to the Ft. Hood killings and the Christmas Day airbomber urge wannabe American jihadis to open fire on crowded restaurants in the nation's capital to massacre U.S. government workers. The advice appears in "Inspire," the latest issue of a slick propaganda publication by Al Qaeda in the Arabian Peninsula (AQAP). "A random hit at a crowded restaurant in Washington, D.C., at lunch hour might end up knocking out a few government employees," a writer

wrote in the 74-page jihadi how-to magazine. “Targeting such employees is paramount and the location would also give the operation additional media attention,” he added. According to a copy of the magazine obtained by the SITE intelligence group, AQAP also urged those bent on murdering for Islam to use everything from pickup trucks to improvised pressure-cooker bombs to kill. Source: http://www.nydailynews.com/news/national/2010/10/11/2010-10-11_terror_threat_to_restaurants_as_al_qaeda_calls_for_attacks_on_government_workers.html#ixzz129cdD3JY

Communications Sector

Security experts fear attack of Comcast botnet notification system. Security experts fear that U.S. Internet Service Provider (ISP), Comcast’s latest botnet notification system will be abused by hackers. Details show in the last few months, Comcast will roll out service called “Constant Guard” to all 16 million subscribers. Customers will receive information about the working of Botnet Identification and Notification service, and data on how hackers circulate malware through e-mails with harmful attachments, and Web links that make botnets out of many infected systems. The botnets are then controlled to circulate spam or initiate distributed denial-of-service attacks made to hit Web sites. Comcast’s plan is being rejected by security experts as they foresee it as an exciting opportunity for forged AV/scareware hackers. A senior security advisor at Sophos cautions that these banners get injected into sites and spam customers with the messages leading them to standard fake AV installers. And customers who get a notice but are using a wireless router behind their cable modem, will not be able to figure out which system is infected with malware. The security experts suggested that ISPs who find infected machines on their networks disconnect the customer’s Internet access until the infection is cleaned up properly. This would reduce botnet traffic tremendously and could make users more aware of good security practices. Also, the disconnection of Internet would immediately capture the user’s attention. Source: http://www.spamfighter.com/News-15219-Security-Experts-Fear-Attack-of-Comcast-Botnet-Notification-System.htm

Half of home Wi-Fi networks vulnerable to hacking. Nearly half of all home Wi-Fi networks in the U.K. could be hacked within 5 seconds, according to CPP. The life assistance company employed the services of an ethical hacker to roam six major cities and use specially developed software to identify home networks that were at risk of “Wi-Fi jacking.” Wi-Fi jacking involves hackers piggybacking on a net connection, which allows them to illegally download files, purchase illegal goods or pornography, or even sell stolen goods, without being traced. It also permits them to view the private transactions made over the Internet, providing them with access to passwords and usernames that can subsequently be used to commit identity fraud. CPP’s research revealed 40,000 home Wi-Fi networks were at risk. CPP also said that despite the fact 82 percent of Web users believe their Wi-Fi connection is secure, nearly a quarter of private wireless networks are not password protected. Furthermore, nearly one in five Web users said they regularly use public networks. During his research, the hacker was able to “harvest” usernames and passwords from users of the public Wi-Fi networks at a rate of more than 350 an hour. He also revealed more than 200 web users unsuspectingly logged onto a fake Wi-Fi network over the course of an hour during the experiment, putting themselves at risk from fraudsters who could harvest their personal and financial information. Source: http://www.networkworld.com/news/2010/101410-half-of-home-wi-fi-networks.html?hpg1=bn

Five countries sign on to DNSSEC. Five country code top-level domains for countries in Latin America and the Caribbean have been digitally signed to enable use of the Domain Name System Security Extensions (DNSSEC). The signing on October 5, done by Afilias Ltd. of Dublin, Ireland a provider of Internet registry and back-end services, will enable validation of DNS query responses. It is part of an effort by the company to deploy DNSSEC to 13 top-level domains by the end of the year. "Rolling out DNSSEC is critical to the future of the Internet," said Afilias' director of strategic partnerships and technical standards. This month's signings bring the total to 53, among about 300 top-level domains, that have been signed or are experimenting with DNSSEC. The country code domains that have recently been signed are .ag, used by Antigua and Barbuda; .bz, Belize; .hn, Honduras; .lc, St. Lucia; and .vc, St. Vincent and the Grenadines. Source: http://fcw.com/articles/2010/10/13/dnssec-adds-five-country-domains.aspx

(Florida) **Thief strips copper wiring from county radio tower in Molino.** Copper wiring valued at over $3,000 was reported stolen October 11 from a county radio tower in Molino, Florida. A technician for CES Team One Communications, the company that maintains the radio tower for Escambia County, told deputies that the theft occurred sometime between September 1 and his service visit October 11 morning. The technician told Escambia County Sheriff's Office investigators that someone cut a gate lock on the fence surrounding the tower, which is located behind the Escambia County Health Department on Highway 29. The thief took two copper bars about three feet in length and cut nine, two-foot sections of copper wire; and ten, six-foot sections. The items were valued at $3,450. According to Escambia County officials, the wiring was part of the tower's electrical grounding system and no county communications systems were taken off the air by the incident. A spokesperson said the missing wiring would place the tower and equipment at a higher risk of damage from lightning, and replacement items are on order. The Escambia County Sheriff's Office investigation into the incident is continuing. Source: http://www.northescambia.com/?p=31289

CRITICAL MANUFACTURING

GM recalls Chevy Impalas on seat belt issue. General Motors Co is recalling 322,409 model year 2009 and 2010 Chevrolet Impala sedans because front seat belts may not be properly anchored, the automaker and federal regulators said October 15. No injuries or fatalities have been reported in cases where the seat belts were not securely anchored or twisted, GM said in a letter to the U.S. National Highway Traffic Safety Administration (NHTSA). GM said it will begin asking its Impala customers later this month to bring the sedans to dealerships for inspection and repair if necessary, free of charge. Through mid-August, GM told NHTSA it had received 32 warranty reports of seat belts having separated from their anchorage. The vehicles involved in the recall were assembled in Ontario, Canada from April 2008 to March 2010, GM said. NHTSA said of the 303,100 Impalas recalled in the United States, about two-thirds of them were 2009 models. Source: http://www.reuters.com/article/idUSTRE69E2S620101015

(Missouri) **St. Louis company to close smelter and clean up lead pollution.** Doe Run Resources Corp. of St. Louis, North America's largest lead producer, has agreed to spend approximately $65 million to correct violations of several environmental laws at 10 of its lead mining, milling and smelting facilities in southeast Missouri, the Justice Department, Environmental Protection Agency and the Missouri Department of Natural Resources announced October 8. The settlement also requires the company

to pay a $7 million civil penalty. As part of the settlement, Doe Run will pay a civil penalty of $7 million for violating a series of environmental laws. The settlement also requires Doe Run to establish financial assurance trust funds, at an estimated cost of $28 million to $33 million, for the cleanup of Herculaneum and several active or former mining and milling facilities. Source: http://www.examiner.com/liberal-in-st-louis/st-louis-company-to-close-smelter-and-clean-up-lead-pollution

Defense/ Industry Base Sector

Cost-cutting imperils National Guard 'air bridge'. Air Force budget cuts are threatening the National Guard's "air bridge" that operates around-the-clock to provide air-to-air refuelings to a steady stream of cargo airplanes crossing the Atlantic Ocean to support the war effort. More than 400 National Guard personnel in Maine, New Hampshire, Pennsylvania, and New Jersey could be told to stand down by month's end, depending on an assessment by the Air Force. That includes 150 in Bangor, Maine. A Maine Senator said the Air Force is trying to cut costs in the Air National Guard. But critics said the cuts make little sense because it would cost more in jet fuel and flying time to bring in active-duty Air Force units from farther away. Source: http://www.wcsh6.com/news/local/story.aspx?storyid=132096&catid=2

Emergency Services

Hazmat fusion center launches interactive web portal. After 3 years of research and development, the National Hazardous Materials Fusion Center (Hazmat Fusion Center) has launched its own Web portal. The soft launch of the public Web site was held in August during Fire-Rescue International. The nationwide release, scheduled for October 15 at the opening session of the HOTZONE Conference in Houston, Texas gives the hazmat community access to the entire portal, including the members-only area and the incident reporting system. The purpose of the Hazmat Fusion Center is to promote hazmat responder safety through a systematic approach to hazmat-response data collection, analyses, and information dissemination. The goal is to provide all hazmat responders — regardless of response discipline — with access to the same vital information in a timely manner. The Web site features training materials, resources, summary incident reports, statistics and trends, news, and general hazmat information. Source: http://ohsonline.com/articles/2010/10/14/10-hazmat-fusion-center-launches-interactive-web-portal.aspx?admgarea=news

(Colorado) **'Terrorist attack' sets the stage.** Douglas County, Colorado led the way for an emergency planning drill that began with a mock hijacking. Douglas County officials October 6 hosted "Operation Neptune," an exercise designed to test the limits of local emergency agencies. The exercise began when domestic "terrorists" stole a chemical tanker from the Foothills Water Treatment Plant in Roxborough, a site selected for its wealth of chemical agents. The 2010 exercise came by way of the Douglas County Local Emergency Planning Committee, which is charged with preparing local responders for an emergency involving hazardous materials. The local committee conducts the drill each year to test its agencies, develop emergency plans and refine response procedures, said the director of Douglas County Emergency Management. The Roxborough location was selected because of the potential for chemical releases from a number of nearby sources including the water treatment plant, the railroad line, which carries tons of hazardous materials, and the highway tanker truck routes of C-470 and Colorado 85. More than 100 emergency responders and public officials from

across Douglas County participated. The drill included participation from the FBI, the National Guard, area schools, three local hospitals and four local fire departments. Source: http://coloradocommunitynewspapers.com/articles/2010/10/12/highlands_ranch_herald/news/14rm_neptune_hr.txt

ENERGY

Why it's hard to crash the electric grid. A new study shows why it would be hard for terrorists to bring down the U.S. electric grid. In March 2010, the U.S. Congress heard testimony about a scientific study in the journal Safety Science. A military analyst worried the paper presented a model of how an attack on a small, unimportant part of the U.S. power grid might, like dominoes, bring the whole grid down. Then, a similar paper came out in the journal Nature in April 2010 that presented a model of how a cascade of failing interconnected networks led to a blackout that covered Italy in 2003. The Safety Science paper came to the "highly counter-intuitive conclusion," that the smallest, lowest-flow parts of the electrical system — say a minor substation in a neighborhood — were likely to be the most effective spots for a targeted attack to bring down the U.S. grid. "That's a bunch of hooey," a co-author of the new study said. Published in the journal Chaos September 28, the new study found just the opposite. Drawing on real-world data from the Eastern U.S. power grid, the it showed "the most vulnerable locations are the ones that have most flow through them." A study coauthor noted that if the government changes its investment strategy to put walls around substations with the least amount of flow, "it would be a massive waste of resources." Source: http://www.sciencedaily.com/releases/2010/10/101012121443.htm

NIST releases smart grid standards. The National Institute of Standards and Technology (NIST) has identified five sets of foundational standards for smart grid interoperability and cybersecurity, furthering the Presidential administration's plan for a next-generation, nationwide utility grid. NIST told the Federal Energy Regulatory Commission (FERC) that the standards — which deal with information models and protocols for reliable and secure grid operations — are available for consideration and adoption by federal and state energy regulators. Together, the next sets of NIST standards are part of efforts identified in FERC's July 2010 Smart Grid Policy Statement. While NIST coordinates development of smart grid standards, FERC is in charge of policy to ensure adoption of them. Developing a nationwide smart grid is a priority for the Presidential administration's goals to cut greenhouse gas emissions through the use of smarter technology. It is also integral to economic recovery plans, as the effort will create jobs. Cybersecurity is such a major concern that utility companies said they plan to invest more than $21 billion in this area over the next 5 years to protect the world's electrical grids, a recent report found. Annual spending on smart grid cybersecurity will more than triple from $1.2 billion last year to $3.7 billion in 2015, according to the report. Source: http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=227800031&cid=RSSfeed_IWK_News

(California) **Police respond to bomb threat.** The Carlsbad Police Department's Communications department received a 911 call about a suspicious container located in front of 4706 Amberwood Court next to a power transformer at 7:30 p.m. October 7.The reporting party stated the container looked like an old ammunition container with military markings on it. Inside the container was another container with tape around it, wires coming out of it, and a cylinder with wires coming out of it. Officers responded and determined that the container could be a bomb and for the safety of the

residents, they evacuated eight residences and called the San Diego County Sheriff's Bomb/Arson to examine the container.The San Diego County Sheriffs' Bomb/Arson investigators conducted a preliminary examination of the container and requested that Tamarack Avenue be closed from El Camino Real to Palisades for both west and eastbound traffic for public safety. They used their robots to open the containers and discovered they were empty. There are no suspects. The Carlsbad Police Department and San Diego County Sheriff's Department are conducting a joint investigation. Source: http://thecoastnews.com/view/full_story/9869292/article-Police-respond-to-bomb-threat-?instance=coast_2nd_top_story

Food and Agriculture

(Wisconsin) **Temperature fluctuation prompts recall from Otto's Meats in Luxemburg.** A Luxemburg, Wisconsin, meat processor is recalling all processed, cooked meats produced this year because they may have been under-processed, state food safety officials said. There have been no reports of illness associated with the products from Otto's Meats, according to a statement released October 11 by the Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP). The company's owner said the voluntary recall is based on a temperature fluctuation noted during a routine inspection October 8 of a single meat sample from the smokehouse. A DATCP public information officer said the voluntary recall was prompted by a thermometer problem on a cooking unit. Subsequent retesting of the meat and thermometers on October 8 checked out fine, the information officer said. All products in the voluntary recall carry Otto's Meats on the label, were made this year and were sold at the Otto's Meats retail store in Luxemburg. Source: http://www.greenbaypressgazette.com/article/20101012/GPG03/10120540/1247

Government Sector (including Schools and Universities)

(California) **Bomb threat empties Visalia courthouse.** A bomb threat early October 12 forced the evacuation of the Tulare County Courthouse in Visalia, California. Authorities learned of the bomb threat about 8:20 a.m., according to the sheriff's department. The building was emptied by about 10 a.m., and a bomb-sniffing police dog from the Farmersville Police Department was called in. No bomb was found and the courthouse reopened at 2 p.m. Source: http://www.fresnobee.com/2010/10/14/2117958/bomb-threat-clears-visalia-courthouse.html

Army Cyber Command stands guard over computer networks. The Army launched the Army Cyber Command (ARCYBER), the service's component of the U.S. Cyber Command, this month, centralizing existing resources in the Army's efforts to protect its global computer networks. The new command brings a number of the Army's cyber resources under one roof. That will ensure that the service's policy, force structure, capabilities development, resources and personnel can securely and effectively work together in cyberspace at the tactical, strategic and national levels, said an Army spokesman. The new command, which incorporates Army organizations such as the Army Network Enterprise Technology Command/9th Signal Command and parts of the 1st Information Operations Command/Land, will be incorporated into ARCYBER. ARCYBER also will oversee the cyber operations of the Army Intelligence and Security Command. ARCYBER's personnel level will exceed 21,000 soldiers and civilians. The new command gives the Army an organization that can plan, coordinate, integrate, synchronize, and conduct cyberspace operations. Source:

http://defensesystems.com/articles/2010/10/15/cyber-defense-army-cyber-command.aspx?admgarea=DS

(Vermont) **Man threatens President Obama.** A 43-year-old Vermont man who threatened to kill the president via his Twitter account and blog will receive a mental health evaluation October 18. At a detention hearing October 14, the suspect, of Rockingham, was permitted temporary release to get an in-person mental health evaluation at the request of the defense. He was indicted and pleaded innocent on one count of knowingly threatening to kill the U.S. President, October 13, in U.S. District Court in Burlington. On August 21, the suspect allegedly sent numerous tweets via his Twitter account, SmellyOlTerriss, which included threats to the President's life. "I am dying inside. And I am plainly stating to you that I am going to kill the president." Throughout the day he seems to have a conversation with himself through his tweets to the White House. "When we kill presidents, what's it like? (Don't forget; still a question)," he tweeted. Source: http://www.reformer.com/localnews/ci_16343686

(Florida) **UNF security breach affects more than 100,000 IDs.** It appears more than 100,000 could be affected by a security breach at the University of North Florida (UNF) in Jacksonville, Florida that involves Social Security numbers. In an e-mail sent to students, UNF said a file may have been accessed by someone outside the country. The file contained personal information of high school and college students, plus anyone else who had expressed interest in the university. UNF said it is notifying the 106,884 people who were affected. About half of them (52,853) had their names and Social Security numbers compromised, and the rest (54,031) had their names and dates of birth compromised, according to UNF. The breach happened sometime between September 24 and September 29. UNF said the computer involved has been isolated, and the university is working with the FBI to determine the cause and intent of the breach. Source: http://www.firstcoastnews.com/news/topstories/news-article.aspx?storyid=171731&catid=3

(Oklahoma) **OU evacuates building following earthquake.** An earthquake southeast of Norman, Oklahoma, October 13, brought calls in from across the state. One of the buildings on the University of Oklahoma campus in Norman was evacuated after concerns of structural damage. Dale Hall Tower was full of students at the time. Crews inspecting the exterior said they believe the cracks were on the building before, but students said they have never noticed them. Oklahoma University officials said as a precaution, they called in a team of structural experts to evaluate campus buildings. All students also received a text message about the quake moments after it happened, letting them know what was going on and that no injuries had been reported. Source: http://www.kfor.com/news/local/kfor-ou-evacuates-building-following-earthquake-story,0,291376.story

GAO: Federal background checks can be risky business. The Office of Personnel Management (OPM) should improve its oversight of federal background investigations to ensure the security of personal information, according to a new audit. A Government Accountability Office (GAO) report released October 7 found OPM's Federal Investigative Service (FIS), which conducts background checks for individuals seeking government employment and security clearances, has limited oversight of privacy regulations designed to protect identifying information collected in those processes. FIS is bound by the 1974 Privacy Act and the 2002 E-Government Act to limit the disclosure and use of personal information and to implement safeguards for protecting that data. It does not monitor investigator

and agency compliance to privacy laws, however, the audit found. According to GAO, the Federal Investigative Service collects large amounts of personal identifying information to conduct background investigations. While OPM has developed assessments to ensure data is used only for specified purposes, it has not updated guidance for officials responsible for implementing processes to address those risks. FIS also has limited oversight of investigators and customer agencies to ensure they are following privacy protection regulations, the report found. Source: http://www.govexec.com/dailyfed/1010/100810l1.htm

(Mississippi) **Miss. Guard probes breach of personnel information.** The Mississippi National Guard is investigating the extent of a security breach after nearly 3,000 active members' personnel records, including Social Security numbers, were posted online for several weeks. The National Guard and AP were notified about the breach by the information privacy director of Liberty Coalition, a Washington-based policy institute. The administrative records belonged to the 155th Brigade Combat Team and were compiled at various times between 2006 and 2008, he said. The files contained 2,674 unique names and 2,672 Social Security numbers. Other breached information included dates of birth, security clearance data, ranks and pay grades, and home and cell phone numbers. A spokesman for the National Guard would not confirm whose files were breached. The files had been online since September 10, posted on the brigade team's Sharepoint Web site, which was insecure and did not require a password to access. The information privacy director of Liberty Coalition believes the breach inadvertently happened when someone uploaded the files to a new computer system. Source: http://picayuneitem.com/local/x1274851776/Miss-Guard-probes-breach-of-personnel-information

(California) **Workers hailed for halting school shooting suspect.** A 41-year-old from Oceanside, California, was arrested October 8 for investigation of attempted murder and remained jailed without bail. Detectives were preparing to present the case to the San Diego County District Attorney's Office for possible charges. Police believe the man armed himself with a .357-magnum revolver, jumped a fence and opened fire toward the crowded playground at Kelly Elementary School in Carlsbad, California. Two girls, ages 6 and 7, were each shot in an arm. Construction workers building a school cafeteria chased the gunman. Police said one man jumped in his pickup truck and rammed the man, knocking him down. He and two other workers held the man for police, authorities said. The gunman was fumbling to reload when he was struck, and his poor gun handling may have saved lives, police said. Source: http://www.google.com/hostednews/ap/article/ALeqM5gpgt5xBUGEXRFmhwZpPGDQ-6pZNQD9IPPJMO0?docId=D9IPPJMO0

(North Carolina) **Homemade bomb found at Catawba College; student charged.** A Catawba College student was arrested October 10 after police say they found him with explosive materials on campus in Salisbury, North Carolina. The 21-year-old suspect was charged with two felony counts of having weapons on campus. Police say that fire crews were called to the campus for a report of smoke in a trash can early October 10. They found what appeared to be a homemade bomb in that trashcan, then found a second bomb in another trashcan. Police said the suspect told firefighters a friend had explained how to make a bomb and he wanted to try it. He was released into the custody of his sister. Source: http://www.charlotteobserver.com/2010/10/12/1756724/homemade-bomb-found-at-catawba.html

Information Technology and Telecommunications

Facebook sued for exposing people's names to advertisers. According to a complaint filed by two Facebook users in California Northern District Court, the company knowingly violated its privacy policy by sharing personally-identifiable information with advertisers. From February 2010, following a Web site update, Facebook began including user IDs and/or usernames in Referer headers, therefore allowing advertisers to identity people who clicked on their adds. Both the user ID and username can be used to access a person's Facebook profile, which contains their name. Knowing these identifiers, advertising companies can build automated scripts to associate people with ad clicks. Source: http://news.softpedia.com/news/Facebook-Sued-for-Exposing-People-s-Names-to-Advertisers-161101.shtml

Anonymous plants pirate flag on MPAA Web site. Hacktivists used DNS cache poisoning to deface a Motion Picture Association of America (MPAA) Web site, according to security analysts. The attack on copyprotected.com — a MPAA Web site that reports violations of the copy protection controls on DVDs and Blu-ray discs — is the latest in a string of assaults against the entertainment business organized by the loosely affiliated Anonymous groups. The defaced page carried the logo of the Pirate Bay after the site itself was the victim of a DNS cache poisoning attack. "Someone managed to hijack the DNS registration for copyprotected.com such that it points to an IP with their own web server displaying their own page," said a security researcher. The server displaying the defacement is run by WareNet. It seems the organization was unwittingly roped into the attack and might itself have been a victim. "I wonder if the Anonymous folks are DDoS'ing WareNet to keep them distracted while they're quietly using a server in WareNet's second IP block for their own purposes," the researcher added. Source: http://www.theregister.co.uk/2010/10/15/mpaa_site_dns_hack/

Tougher data protection laws could force businesses to rethink compliance. Data protection laws are expanding worldwide and cracking down on the way businesses protect electronic information, said a new report published the week of October 11. "A New Era of Compliance: Raising the Bar for Organizations Worldwide," written by RSA and the Security for Business Innovation Council (SBIC), analyzes how new legislation and more legal muscle behind regulations are forcing businesses to change how they approach compliance. The report highlights how tougher enforcement, more data breach notification laws emerging around the globe, more prescriptive regulations, and increasing requirements for making enterprises responsible for the security of their data even when a business partner handles it are requiring businesses to look at compliance as a strategy, not just a necessary evil. In the report, the SBIC offered several recommendations for enterprise security teams in what it calls a new era of compliance. Source: http://www.darkreading.com/security/management/showArticle.jhtml?articleID=227701206&subSection=Security+administration/management

Former White House advisor wants cybercrime haven crackdown. A former White House security advisor has urged a crackdown on rogue states that serve as a "safe haven" for cybercrime, along with a fundamental rethink of Internet architectures. He told delegates to the RSA Conference in London, England that Western law enforcement officials often fail to get the help they need when after they track back the source of cyber attacks to countries such as Moldova, Russia, and Belarus in eastern Europe. "These countries are international cyber-sanctuaries for crime," he said. He said

"renegade" countries need to be pressured into acting on cyber-criminals through a process akin to the way in which countries who tolerated the laundering of drug profits through their banking system were brought into line. The former security adviser argued that a fundamental rethink on Internet architectures was needed in order to limit cybercrime and related problems, such as economic espionage. "Spending more money on firewalls, anti-virus and intrusion prevention is just throwing more good money after bad," he said. "The money spent to develop the next version of the X-box would be better spent on the next protocol for the Internet." Source: http://www.theregister.co.uk/2010/10/14/clarke_cybercrime_rsa/

Microsoft fixes record 49 holes, including Stuxnet flaw. In a record Patch Tuesday, Microsoft released updates October 12 for Windows, Internet Explorer, and the .NET framework that feature fixes for 49 holes, including one being exploited by the Stuxnet worm. The release plugs one (MS10-073) of the remaining two holes, and the company said in a blog post that the final hole will be addressed in an upcoming security bulletin. Meanwhile, Microsoft provided a priority list for the 16 bulletins being released, which fix 6 holes that are rated "critical." Four vulnerabilities are singled out because there are likely to be exploits developed for them, according to a Microsoft blog that assesses the risks of the various vulnerabilities. Source: http://news.cnet.com/8301-27080_3-20019353-245.html

Two million U.S. PCs recruited to botnets. The United States leads the world in numbers of Windows PCs that are part of botnets, reveals a 240-page Microsoft report. More than 2.2 million U.S. PCs were found to be part of botnets in the first 6 months of 2010. Brazil had the second highest level of infections at 550,000. Infections were highest in South Korea where 14.6 out of every 1,000 machines were found to be enrolled in botnets. The report took an in-depth look at botnets which, said the head of security and identity at Microsoft U.K., now sit at the center of many cybercrime operations. A botnet called Lethic sent out 56 percent of all botnet spam sent between March and June even though it was only on 8.3 percent of all known botnet IP addresses. In the 3 months between April and June 2010, Microsoft cleaned up more than 6.5 million infections, which is twice as much as the same period in 2009. The statistics in the report were gathered from the 600 million machines that are enrolled in Microsoft's various update services or use its Essentials and Defender security packages. Source: http://www.bbc.co.uk/news/technology-11531657

Most large companies hit by hack attacks, survey shows. A survey of 350 IT and network professionals would indicate that 2010 has been worse than 2009 for getting hacked, with large companies in particular reporting this to be worse than last in terms of suffering at least one network intrusion of their user machines, office network, or servers. The Sixth Annual Enterprise IT Security Survey, released October 11, found that 67 percent of large companies with 5,000 or more employees reported one successful intrusion or more this year, compared with 41 percent in 2009. Mid-size companies of 1,000 to 4,999 employees fared better with 59 percent reporting an intrusion, up slightly from 57 percent in 2009. For the first time, the survey, sponsored by VanDyke Software and undertaken by Amplitude Research in mid-September, delved into what the survey respondents believed primarily caused the network intrusion. Fourteen percent of those surveyed attributed their intrusion problem to "hacker/network attack," 12 percent cited "lack of adequate security policies/measures," 10 percent said "employee Web usage," 9 percent pointed to "virus/malware/spyware," 8 percent faulted other "employee carelessness, negligence," 6 percent said "unauthorized access by current/former employees," 5 percent blamed "weak passwords," 5

percent thought it was because of "lack of software updates," and 5 percent simply said "software security flaw/bug." Source:
http://www.computerworld.com/s/article/9190559/Most_large_companies_hit_by_hack_attacks_survey_shows

University study offers recipe for stealth malware attacks via social networks. A group of researchers the week of October 4 published a paper that mathematically shows how a low-and-slow malware attack based on social networking behavior patterns could be more effective than a traditional network attack. In their paper, Stealing Reality, researchers from MIT, Ben Gurion University, and Deutsche Telekom Laboratories offer formulas that show the potential effectiveness of a "stealth" attack that uses social networks as its underlying platform. "In this paper we discuss the ability to steal vital pieces of information concerning networks and their users by a nonaggressive — and hence, harder to detect — malware agent," the researchers say. "We analyze this threat and build a mathematical model capable of predicting the optimal attack strategy against various networks." The paper offers a number of mathematical models conducted on actual mobile network data, showing that malware attacks can be adapted to follow human behavior on social networks. Source:
http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=227701108

Experts: Stuxnet a "game changer". The Stuxnet malware is a game changer for critical information infrastructure protection, an EU security agency has warned. ENISA (European Network and Information Security Agency) issued a technical report titled "Stuxnet Analysis," in which it warns that a similar attack of malware capable of sabotaging industrial control systems as Stuxnet may occur in future. A researcher writes that the worm, whose primary method of entry into systems is infected USBs, essentially ignores vulnerable Windows boxes but aggressively attacks industrial control (SCADA) systems from Siemens, establishing a rootkit as well as a backdoor connection to two (now disconnected) command and control servers in Malaysia and Denmark. PLC controllers of SCADA systems infected with the worm might be programmed to establish destructive over/under pressure conditions by running pumps at different frequencies, for example. The researcher notes there is no evidence either way as to whether this has actually happened. Source:
http://homelandsecuritynewswire.com/experts-stuxnet-game-changer

'Scrapers' dig deep for data on Web. At 1 a.m. on May 7, the Web site PatientsLikeMe.com noticed suspicious activity on its "Mood" discussion board. There, people exchange highly personal stories about their emotional disorders, ranging from bipolar disease to a desire to cut themselves. It was a break-in. A new member of the site, using sophisticated software, was "scraping," or copying, every single message off PatientsLikeMe's private online forums. PatientsLikeMe managed to block and identify the intruder: Nielsen Co., the privately held New York media-research firm. Nielsen monitors online "buzz" for clients, including major drug makers, which buy data gleaned from the Web to get insight from consumers about their products, Nielsen says. The market for personal data about Internet users is booming, and in the vanguard is the practice of "scraping." Firms offer to harvest online conversations and collect personal details from social-networking sites, resume sites, and online forums. Scrapers operate in a legal gray area. Internationally, anti-scraping laws vary. In the United States, court rulings have been contradictory. Source:
http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html?mod=WSJ_hpp_MIDDLETopStories

Trojan forces Firefox to secretly store passwords. A Trojan recently analyzed by Webroot is said to rely on retrieving Web page passwords from a browser's password storage, rather than logging a user's keyboard inputs. To make sure it will find all the interesting passwords in Firefox, the malware, called PWS-Nslog, makes some changes to jog the browser's memory. A few manipulations in a JavaScript file prompt Firefox to store log-in information automatically and without requesting the user's consent. The malware will, for instance, simply comment out Firefox's confirmation request in the nsLoginManagerPrompter.js file and add a line with automatic storage instructions. The H's associates at heise Security were able to reproduce the effect of the manipulations, which the malware author probably borrowed from a work around that has been in circulation since 2009. The manipulation works on all platforms on which the Trojan has the rights to modify the nsLoginManagerPrompter.js file. In tests, this worked on Windows XP, Windows 7, and Ubuntu 10.04. However, on Windows 7 and Ubuntu the user is usually working with limited privileges by default, and under these circumstances the malware is unable to manipulate the file. According to Webroot, the malware author did not put any effort into covering his tracks, as the malware contains a name as well as a Gmail address. Furthermore, Webroot soon found the Facebook page of the allegedly Iranian developer who claims he develops crimeware for fun. Source: http://www.h-online.com/security/news/item/Trojan-forces-Firefox-to-secretly-store-passwords-1106100.html

National Monuments and Icons

(New York) **Explosives at N.Y. cemetery more than 13 years old.** The military-grade explosives found at a historic New York City cemetery are more than 13 years old, police said October 12. It was still unclear who placed the plastic bag of C-4 at the foot of a tombstone in New York City Marble Cemetery on Manhattan's Lower East Side. A caretaker planting shrubs in the cemetery dug up the bag in May or June 2009, did not realize what it was and left it. It remained in the back, near a tree, until a volunteer saw it over the weekend of October 9 and 10 and put it in a trash can, thinking it was a leftover movie prop because the cemetery is often used as a film setting, police said. But the volunteer thought it might be dangerous and called police October 11. The discovery caused a bomb scare and shut down the area until police determined it could not detonate. The grave at which the bag was found was dated 1919. The cemetery, which was designated a landmark in the 1960s, is usually closed to the public. Source: http://www.google.com/hostednews/ap/article/ALeqM5itXvQmi2gbDJMqfqV7joCj_ghF2AD9IQDJ880?docId=D9IQDJ880

(Wyoming) **Antelope Fire continues to dwindle in park near Mt. Washburn.** The Antelope Fire in Wyoming grew to 5,510 acres over the week of October 4, but cooler, moist weather is diminishing fire activity. Yellowstone Park fire officials are expecting little in fire movement or progression though the week and are primarily monitoring it, with one engine and seven firefighters assigned to the fire. The fire, which is located northeast of Mt. Washburn south of the Tower Falls area in the north-central portion of the park, was measured at 5,510 acres October 5. It is now listed as 20 percent contained. Source: http://www.westyellowstonenews.com/news/article_bde40842-d3c2-11df-8ef6-001cc4c002e0.html

Postal and Shipping

GAO calls for better cargo data analysis. U.S. Customs and Border Protection (CBP) should establish a timeline for determining how to assess potential threats posed by the contents of U.S.-bound cargo containers using data collected on individual containers since January, the Government Accountability Office (GAO) concluded in a report made public October 12. The Importer Security Filing and Additional Carrier Requirements call for collection of 10 pieces of information on U.S.-bound cargo containers, including their country of origin, and two additional pieces of information on ships carrying the cargo. The regulation, referred to as the "10+2 rule," was put in place to meet a Congressional mandate that additional cargo data cargo be collected to help prevent illicit transfers of weapons of mass destruction and other controlled materials. A CBP assessment of the requirements fails to specify why the federal office had chosen to collect the specific pieces of information over other proposals considered, the report stated. Investigators recommended "that CBP should, if it updates its regulatory assessment, include information to improve transparency and completeness, and set time frames and milestones for updating its national security targeting criteria." GAO said DHS "concurred with these recommendations." Source: http://www.globalsecuritynewswire.org/gsn/nw_20101013_9793.php

(Texas) **Amid white powder scare, HISD sets new mail rules.** The Houston school district has imposed strict rules for handling incoming mail after more schools October 11 discovered typewritten envelopes containing a suspicious, but unharmful powder. On October 8, 13 schools in the Houston Independent School District received the envelopes. More envelopes were discovered by school officials at four other schools October 9 and 11. A field test done October 8 by the Houston Fire Department's hazardous material unit indicated that the substance was cornstarch. The incident, while serious, had little impact on overall operations at the campuses. FBI officials believe each envelope is connected to an individual or a group of individuals. School officials have put in place new procedures for handling mail. All mail now must be screened and opened in an isolated area, and if an item is suspicious, the air handlers must be turned off, and the room must be evacuated and secured, said an HSID spokesperson. In addition, the person who handled the mail must be isolated, and the police should be notified, she said. School personnel also are being advised to open mail before or after school hours. The U.S. Postal Inspection Service also has implemented a special screening process for all HISD mail. Source: http://www.chron.com/disp/story.mpl/metropolitan/7242301.html

Public Health

(Washington) **Bomb squad blows up suspicious bag at hospital.** A bomb squad blew up a suspicious bag left in an employee parking lot October 13 at Deaconess Medical Center in Spokane, Washington. The Spokane Explosive Device Unit detonated the bag at Fifth Avenue and Monroe Street to the west of the hospital. When an employee parked his car in the gravel employee lot, he noticed the bag next to a concrete barrier near the alley between Fourth and Fifth avenues. He immediately notified Deaconess security, who called the Spokane Police Department. Officers responded just after 8 a.m. and locatedthe bag. A police spokeswoman said there was not a threat, but a suspicious bag, whiccould have simply been discarded or left behind. Police did not want to take chances because

there were suspicious signs on the bag, which officers declined to specify, shesaid. The bomb squad about 10:30 a.m. deployed a robot to the collect the bag for a safe disposal. d , s e h n e . e h Source: http://www.spokesman.com/stories/2010/oct/13/monroe-street-shut-down-police/

CareFusion recall classified as most serious type. The Food and Drug Administration has classified CareFusion Corp's August recall of 17,000 Alaris medication pumps as a Class I recall, the most serious type, the company said October 15. A Class I recall is a situation in which there is a reasonable probability that the product will cause serious health consequences or death. CareFusion said it is working to correct the problem by updating hardware on the pumps, which are used to infuse medication into a patient's circulatory system, and has recorded a reserve in its fiscal fourth quarter to complete remediation. On August 24, CareFusion recalled the Alaris PC model 8015 manufactured or serviced between December 2008 and September 2009. It said the pump could experience intermittent communication errors under certain wireless network conditions, freezing the pump's screen and possibly delaying therapy. If the communication error occurs during infusion, infusion continues as originally programed but cannot be modified. When this occurs, stopping infusion to make any modification or programing changes causes the pump to shut down, with a delay in therapy, which could lead to serious injury or death. Source: http://www.reuters.com/article/idUSTRE69E2DQ20101015

Pfizer recalls nearly 200K bottles of Lipitor. Pfizer is recalling 191,000 bottles of Lipitor, the popular cholesterol-lowering drug, after the pharmaceutical company received complaints of an unusual odor emanating from the meds. Pfizer said health problems related to the smell are unlikely. The drug company and the bottle supplier are investigating the source of the odor. Each bottle contains 90 Lipitor tablets in a 40-milligram dose. The recall includes the following five lots of Lipitor bottles in the U.S.: 0855020, 0819020, 0842020, 0843020, and 0854020. Source: http://abclocal.go.com/kabc/story?section=news/consumer/recalls&id=7718544

More testing advised for biowatch program. An expert committee has recommended additional testing to verify the value of a nationwide system for alerting the U.S. government of airborne biological threats, the National Academies' Institute of Medicine announced this month. The Biowatch program was established in 2003 by the Homeland Security Department and encompasses air testing devices fielded in more than 30 urban areas. Air samples are collected each day from the devices and are tested for the presence of biological warfare materials such as smallpox and anthrax. DHS, following a request from Congress, asked the National Research Council and the Institute of Medicine 2 years ago to establish a panel to investigate the efficacy of the present Biowatch effort. A new report brief summarizing the panel's findings highlights multiple areas of concern over the operation and priorities of the Biowatch system. These include a lack of complementariness between the federal effort and local and state public health programs found to be more adaptable and wide-ranging in their ability to detect infectious pathogens. Source: http://www.globalsecuritynewswire.org/gsn/nw_20101012_3712.php

(New Hampshire) **FBI responds to hospital threat.** On October 8, an FBI agent and a state bomb-sniffing dog team did a sweep on the property of Concord Hospital in response to threats made to the hospital, said a supervisory special agent to FBI officers in New Hampshire. He declined to discuss the nature of the threats. The hospital "felt that at the time the threats warranted some precautionary measures and getting law enforcement involved," he said. The search of the hospital grounds turned

up nothing, said the hospital's vice president for community affairs. Staff were told of the search so as to allay any fears of visitors or patients, she said, and there have been no problems since. Source: http://www.concordmonitor.com/article/219798/fbi-responds-to-hospital-threat

Transportation

(New York) **Airplane stolen from Steuben County airport.** The Steuben County Sheriff's Office is investigating the theft of a small airplane from the Hornellsville, New York, Municipal Airport. Police said the single-engine 1964 Cessna 150 D, registration N43ED, was stolen about September 20, and was noticed missing from the hanger October 4. The incident was reported October 11, after the owner was notified by airport employees that the plane was no longer there. The aircraft had been advertised for sale since June and airport employees assumed the aircraft had been sold, the sheriff's office said. The sheriff's office is working with the Elmira FBI field office and other jurisdictions to locate the stolen airplane. Source: http://www.democratandchronicle.com/article/20101013/NEWS01/101013035/1002/NEWS

(Nevada) **Bus evacuated north of Reno after bomb scare.** Transportation officials said 18 passengers were evacuated from a Regional Transportation Commission (RTC) bus in Stead, Nevada, October 12, after an unknown suspect allegedly threw a backpack onto the vehicle, yelled "bomb" and ran away. The Reno Police Department closed Stead Boulevard at Silver Lake Road while it investigated the incident that occurred at about 8:15 p.m. Officers would not speak with reporters about the incident, but a RTC spokeswoman confirmed the evacuation and the threat. The bomb squad also responded, according to a photographer on scene. Source: http://www.mynews4.com/story.php?id=29524&n=122

Water and Dams

Chemicals survive waste treatment to be released into environment: study. Chemicals in household drugs and cleaning products routinely survive waste treatment and are released into the environment, where little is known about their effects on land, water, and human health, according to a study funded by the Canadian government. "What are really needed are risk assessments," said a research consultant who conducted the study for the Canadian Council of Ministers of the Environment. "The whole ecosystem needs to be assessed for the effects of the materials that are present." He looked at treatment in 11 Canadian communities from coast to coast. He analyzed sludge entering the system and "biosolids" at the end that are often spread on fields or used in land reclamation. His study looked for 82 different chemicals, including bisphenol A, which was declared a toxic substance October 13. Two dozen of the compounds were still present in more than half the treated samples. Bisphenol A remained in 86 percent of treated samples at an average concentration of 325 parts per billion. Triclocarban, an antibacterial agent found in soap and disinfectant and known to cause hormone disruption in rats, was found in all treated samples. The mood-stabilizing drug Carbamazepine was also found in low levels in all samples. Antibiotics, anti-fungal agents, fragrance compounds, and painkillers survived treatment in more than two-thirds of samples. He said it is hard to say to if any chemicals reached dangerous levels. Safe levels have not been set for many of them. Source: http://www.winnipegfreepress.com/life/sci_tech/chemicals-survive-waste-treatment-to-be-released-into-environment-study-104965919.html

(New York) **EPA to excavate contaminated soil, monitor groundwater at Ellenville Scrap Iron and Metal Superfund site.** The U.S. Environmental Protection Agency (EPA) announced October 12 that it has finalized the steps it will take to clean up the Ellenville Scrap Iron and Metal Superfund site in the Ellenville, New York, in Ulster County. EPA will excavate contaminated soil from six different areas at the site, consolidate the soil on the landfill portion of the site, and then securely cap the landfill, which will prevent further contamination of the groundwater. Any of the excavated soil or materials that are characterized as hazardous waste will be shipped off-site for proper disposal. EPA will also install a series of additional wells to monitor groundwater around the site to make sure it remains free of contaminants. Source: http://yosemite.epa.gov/opa/admpress.nsf/0/d60a7528e589ca85852577ba005e701d?OpenDocument

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**